

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

GLOBERANGER CORPORATION	§	
	§	
Plaintiff,	§	
	§	
v.	§	CIVIL ACTION NO. 3:11-CV-0403-B
	§	
SOFTWARE AG,	§	
SOFTWARE AG USA, INC., NANIQ	§	
SYSTEMS, LLC, and MAIN SAIL LLC,	§	
	§	
Defendants.	§	

MEMORANDUM OPINION AND ORDER

Software AG USA, Inc. and Software AG, Inc. (together, “SAG”), joined by Naniq Systems LLC (“Naniq”) (collectively, “Defendants”),¹ move for summary judgment on Plaintiff GlobeRanger Corporation’s (“GlobeRanger”) four state law claims, which include trade secret misappropriation, tortious interference with a contract, unfair competition, and conspiracy. Having conducted a lengthy review of the parties’ briefing and submissions, the Court finds summary judgement appropriate solely for GlobeRanger’s tortious interference claim. Accordingly, the Court **GRANTS IN PART** and **DENIES IN PART** Defendants’ Motions for Summary Judgment (docs. 135, 138).

I.

BACKGROUND

This case centers on Defendants’ alleged misappropriation of GlobeRanger’s radio frequency identification (“RFID”) technology. GlobeRanger installed the RFID solution at issue for the U.S.

¹ Main Sail LLC (“Main Sail”) was dismissed from this case on May 13, 2014 (doc. 151) while Defendants SAG’s and Naniq’s Motions for Summary Judgement were pending.

Navy (the “Navy Solution”)² as part of a subcontract signed in 2007. GlobeRanger claims that SAG improperly gained access to the Navy Solution while working on a subsequent RFID project for the Navy, and that SAG used this access to reverse-engineer its own commercial RFID solution. SAG now argues in its Motion for Summary Judgement that its actions were lawful because the Navy had the right to disclose the Navy Solution under federal procurement regulations. The facts pertinent to this analysis, gleaned from the summary judgment record, are as follows.

A. *RFID Technology*

RFID is wireless technology that uses radio wave signals for the purpose of automatically identifying and tracking objects. This automatic identification system starts with RFID “tags” and “readers.” The tag is attached to the desired object and stores information, such as “identification numbers, location, or specifications of the tagged product.”³ The reader emits radio waves that signal tags, as they come in range, to automatically send back their stored data, which the RFID reader “then relays to a computer system installed with identification software.”⁴

New technological developments over the past three decades have led commercial and government entities to adopt RFID across various applications, including electronic highway toll collectors, employee ID cards, and automatic payment systems.⁵ Relevant to this analysis, RFID

² For ease of reference, the Court calls the package of RFID technology that Defendants allegedly accessed in stealing GlobeRanger’s trade secrets the “Navy Solution.” In reality, Defendants appear to have accessed at least two different solutions that GlobeRanger implemented for the Navy.

³ Justin M. Schmidt, *RFID and Privacy: Living in Perfect Harmony*, 34 RUTGERS COMPUTER & TECH. L.J. 247, 250 (2007).

⁴ *Id.* at 249–50.

⁵ *See id.* at 255–57.

technology has become a powerful inventory management tool for many organizations. It allows enterprises to tag inventory as it arrives, automatically track that inventory as it moves within warehouses or to new facilities and eventually to the end-users. The enterprise can use the data its RFID readers automatically compile in a central computer system to analyze customer spending and automate business processes like inventory re-ordering.

B. GlobeRanger's Development and Protection of its RFID Solution

Established in 1999, GlobeRanger is a small Texas-based company that has spent years implementing automatic identification technology for both private and government customers. In the early 2000s, GlobeRanger was hired by companies that include Anheuser Busch, Ford Motor Company and John Deere to install automatic identification systems for purposes such as asset tracking and warehouse inventory processing. (Pl.'s App., Doc. 146, at 1–7, 415.) In the mid-2000s, GlobeRanger's business improved markedly after the Department of Defense ("DoD") issued a series of mandates requiring all DoD entities to implement RFID technology in an effort to improve inventory logistics.⁶ The record shows GlobeRanger subcontracted⁷ on various RFID projects aimed at complying with these DoD mandates.

The most prominent example of GlobeRanger's work for the DoD was the RFID solutions it installed for the Defense Logistics Agency ("DLA"), an agency tasked with acquiring goods and supplies from commercial suppliers and distributing those goods and supplies to U.S. and foreign

⁶ See Sheila C. Stark & Euza P. Nagle, *Full Speed Ahead with DoD Identification Requirements: Next Stop, Radio Frequency Identification*, PROCUREMENT LAW., Fall 2004, at 11, 11.

⁷ The government often contracts directly with "prime" contractors, who then enter into contracts with subcontractors to carry out more discrete tasks.

military services. GlobeRanger performed this work pursuant to its non-exclusive resale agreement that it signed in 2005 with Psion Teklogix (“Psion”). This agreement made Psion—an RFID hardware manufacturer—a non-exclusive reseller of GlobeRanger’s RFID products and services to government agencies. (*See id.* at 8–18.) Under this agreement, GlobeRanger implemented RFID solutions at various depots operated by the DLA starting in 2005. (*Id.* at 19–21, 416–17.) And since the DoD’s mandate required commercial suppliers to integrate with these RFID systems, GlobeRanger sold similar RFID solutions to DLA suppliers, including Honeywell Aeupace and Sopacko Packaging. (*Id.* at 62–66, 336, 417.) By 2007, an industry analyst noted that “GlobeRanger currently has over 89 deployments of its [RFID technology].” (*Id.* at 67.)

GlobeRanger benefitted from this widespread deployment of its RFID technology across various enterprises. It “provided GlobeRanger with the knowledge of how to deploy and orchestrate a myriad of types and brands of hardware” and the ability to “integrate” its technology “with enterprise business systems . . . and automate enterprise business processes.” (*Id.* at 416.) This experience led to the development of GlobeRanger’s “proprietary RFID Solution,” which it calls the “GlobeRanger Solution.” (Pl.’s Br. Supp. Resp. (“Pl.’s Resp.”), Doc. 145, at 1.)

The GlobeRanger Solution is a package of RFID technology that GlobeRanger developed and assembled to license to customers.⁸ At the GlobeRanger Solution’s core is the iMotion platform, which is a combination of software and other components that GlobeRanger has licensed to

⁸ GlobeRanger does not explicitly define the GlobeRanger Solution in its brief, and at times, describes it in vague terms. This appears to stem, in part, from the fact that GlobeRanger was continually improving its RFID technology over the course of its existence, such that its core package of RFID technology differs somewhat across different periods of time.

customers since 2001 for tracking and processing purposes.⁹ (Pl.’s App. 337, 414–15.) GlobeRanger later developed and added Solution Accelerators and Expansion Packs to round out its GlobeRanger Solution. Though not clearly defined, Solution Accelerators and Expansion Packs appear to be packages of technology that are added to the iMotion platform to perform certain functions, such as integrating and communicating with the RFID technology or the enterprise’s computer systems. (See *id.* at 336–39, 415.) Functionally, the GlobeRanger Solution filters raw RFID reads “into meaningful business events, on a real time basis, through four layers,” starting with the device adapter and ending with a workflow, which “is a series of instructions or rules telling a computer what to do in response to various inputs.” (*Id.* at 415–16.)

The GlobeRanger Solution is not a one–size–fits–all product; it must be molded according to each customer’s RFID needs and computer systems. This customization includes adding “components, workflows, and business processes,” with the end product being a custom RFID “solution.” (*Id.* at 414.) For example, the Navy Solution, discussed in more detail later, was built using the GlobeRanger Solution as its base and adding customized features unique to the Navy that may differ from those GlobeRanger built into the “Daisy Solution” for Daisy Brand. (*Id.* at 417.)

Ultimately, GlobeRanger spent over \$30 million to develop the GlobeRanger Solution. (*Id.* at 414.) To protect its investment, GlobeRanger requires that users “review and click ‘agree’ to the terms of” GlobeRanger’s End User License Agreement (“EULA”) before that solution may be activated or moved to a different device. (*Id.* at 426.) Under its EULA, GlobeRanger retains all intellectual property rights in its solution, and prohibits disclosure of its product without

⁹ (See, e.g., Pl.’s App. 14–15 (describing, in GlobeRanger’s agreement with Psion, the iMotion platform as including various software and other components).)

GlobeRanger's written consent.¹⁰ GlobeRanger also uses license keys that are both device specific and node-locked, which "means that once a license file is activated, the program cannot be moved to a different device, or the program will lock" until a new license is activated. (*Id.*) GlobeRanger's further protects its information by making employees sign non-disclosure agreements ("NDAs") when hired, and requiring employees to sign certifications that all confidential information has been returned upon severance. (*Id.* at 419.) GlobeRanger similarly requires contractors working on its solutions to sign NDAs agreeing not to disclose or claim title to GlobeRanger's intellectual property. (*Id.* at 419.)

C. *Events Preceding the Alleged Misappropriation*

In 2005, the Navy entered into contracts with prime contractors CACI International, Inc. ("CACI") and Science Applications International Corp. ("SAIC") to assist in implementing an RFID system per the DoD's RFID mandate. (*See* Def.'s App., Doc. 137, at 196–240, 379–393.) SAIC, in turn, entered into a renewable subcontract with GlobeRanger, in 2007, providing that GlobeRanger would participate in the implementation of RFID solutions at selected sites. (*See id.* at 86–115.) Pursuant to its subcontract, GlobeRanger built and implemented the Navy Solution at three different Navy locations: Kanehoe Bay ("K-BAY"), Pearl Harbor, and San Diego. (*Id.* at 51.)

By 2008, the Navy decided to implement a centralized, enterprise-wide RFID system to cover 700 different sites. (*Id.* at 138.) To evaluate what platform to use in building this enterprise-wide RFID solution, an Architecture Evaluation Team was assembled. (*Id.* at 117.) Led by the Navy's

¹⁰ (*See* Pl.'s App. 9–10 ("All such U.S. Federal Government end-users shall not provide or otherwise make available the Software or documentation, or any portion thereof, in any form to any third party without the prior written approval of [GlobeRanger].").)

Robert Bacon, the Team included two additional Navy employees and six representatives from the Navy's various contractors, including two consulting firms later named as defendants in this case, Main Sail and Naniq.¹¹ (*Id.*) The Architecture Evaluation Team limited its assessment to just two products/companies: the GlobeRanger Solution and SAG's webMethods. (*Id.* at 126, 156, 162.)

SAG consists of two U.S. subsidiaries of the German technology company Software AG.¹² SAG's software suite, webMethods, was apparently chosen as one of the candidates for the Navy's enterprise-wide RFID project because of the Navy's familiarity with webMethods on prior projects. (*Id.* at 156.) Additionally, webMethods is a leading middleware product, capable of linking numerous systems to a central location. But as SAG admits, webMethods had never been used for the specific purpose of enabling an RFID system. (Pl.'s App. 213–18.) Likewise, SAG essentially had no experience implementing RFID technology before the Navy's evaluation process began. (*Id.*)

Nevertheless, after an extended process, the Architecture Evaluation Team issued a report in February 2009 recommending SAG's webMethods. (Def.'s App. 126–30.) The Navy considered this report, and in November 2009 expressed approval by entering into a contract with SAG concerning the implementation of an RFID solution using webMethods as a platform. (*Id.* at 267–94.) Meanwhile, the Navy ordered GlobeRanger to stop its RFID subcontracting work on October 9, 2009, and informed GlobeRanger that the Navy's three existing RFID sites would be “converted to the new RFID Enterprise Architecture Solution next calendar year.” (*Id.* at 172.)

¹¹ As mentioned, Main Sail, who did not seek summary judgment, was dismissed from this case after settling with GlobeRanger. Naniq, who involuntarily dissolved in 2011, joined in SAG's Motion.

¹² Software AG, the publically-trade German technology company, was dismissed from this case on April 12, 2013 due to lack of personal jurisdiction. (See Doc. 71.)

D. *The Alleged Misappropriation*

Pursuant to its contract with the Navy, SAG supported the Navy's RFID Asset Visibility Enterprise ("RAVE") project team, which included, among others, Bacon and representatives from Naniq and Main Sail. GlobeRanger submits evidence purportedly showing that SAG wrongfully accessed the Navy Solution during the RAVE project in at least three ways.¹³

First, Defendants and the Navy's Bacon allegedly misrepresented their intentions to GlobeRanger in order to access and copy images of the Navy Solution on two different occasions so that SAG could study and reverse-engineer its own solution using webMethods as a platform. The first of these images was made around September 2009, when Naniq copied an image of the Navy Solution that GlobeRanger had installed for the Navy at K-BAY. Naniq was able to do this because of an email in which Bacon requested a license key, claiming that Naniq would "be coming by to see the GR server for routine maintenance and to take a scan." (Pl.'s App. 227.) In sending a license key to Naniq, GlobeRanger reminded it, among other things, that "the use of such license keys and GlobeRanger Software shall be limited to the direct support of the Navy's existing installation of GlobeRanger Software and for no other purpose otherwise be subject to the terms of the GlobeRanger [EULA]." (*Id.* at 239.) And while Main Sail, unlike Naniq, was not under contract to help with the Navy Solution at K-BAY, Main Sail's representative sent emails trying to help Naniq unlock the Solution at K-BAY and following up to ensure the key was received. (*See id.* at 228–29, 232–33.) After receiving this key, Naniq confirmed that it was able to capture "a fully functioning

¹³ The Court does not explore a fourth potential source—GlobeRanger's partial data dictionary. GlobeRanger never mentions the partial data dictionary in its facts detailing Defendants' "theft," and never presses it as a source in which Defendants acquired its trade secrets, even though it mentions the data dictionary in its pleadings as a source SAG used to discover the trade secrets.

image of the server at Kbay.” (*Id.* at 228.)

The second of these images was made in January 2010, when Naniq again copied an image of the Navy Solution, this time at Pearl Harbor. In this instance, Naniq obtained the key directly from a GlobeRanger representative through an email exchange on January 8, 2010. (*Id.* at 243.) In it, Naniq claimed it simply needed the key to run maintenance on the K-BAY solution. (*Id.*) That same day, Main Sail sent an email confirming Naniq was “ready to install a copy of GlobeRanger with the Pearl configuration on a windows server provided by” the Navy. (*Id.* at 248.)

Subsequently, the RAVE team can be seen openly discussing what they were using these images for. Naniq, for example, discussed how RAVE team leader Bacon “is interested in having [Naniq] come into the Lab next week and load the GlobeRanger instances currently implemented at Navy sites on either a windows XP or Windows Server box.” (*Id.* at 246.) Naniq further noted that the RAVE team wanted to “demonstrate how [they] can access these instances to better understand the [Navy Solution’s] workflows, legacy systems, integration, and reporting. This will provide the ability to reach into the current solution at various locations and duplicate this effort in webMethods in the lab environment.” (*Id.*) Bacon similarly wrote that “getting the exact instances of what we have running with GR loaded into a workstation will streamline the development/conversion process This should be very beneficial to [the Navy] and WebMethods.” (*Id.* at 246.) A presentation from the RAVE team indicates that these images had been loaded onto servers in designated labs. (*Id.* at 251.) This presentation even notes that one of the RAVE team’s goals is to “[r]eplicate current GlobeRanger functionality.” (*Id.* at 276.) And at an RFID conference in April 2010, Bacon, when asked publically about the Navy’s RFID project, openly admitted: “We had a jump start because we had already . . . implemented [the other sites] using GlobeRanger servers on every site.

So we sort of had that in our hip pockets which helped us jump start webMethods because we just reverse engineered code from GlobeRanger—which saved us.” (*Id.* at 323.)

Second, SAG also purportedly had access to GlobeRanger’s proprietary information through technical manuals that were delivered with the Navy Solution. (*See* Def.’s App. 341–67.) These manuals apparently helped SAG discover, among other things, GlobeRanger’s Business Processes and Architecture. (*See* Def.’s Br. Supp. Mot. Summ. J. (“Def.’s Mot.”), Doc. 136, at 14 nn. 13, 14.) GlobeRanger defines its Business Processes as the “secret sauce” that allows the “software and hardware components of RFID work in harmony,” telling the RFID system, among other things, what it “should do about” raw RFID reads that the reader picks up. (First Am. Compl. (“FAC”), Doc. 79, ¶ 15.) Its Architecture is “the blueprint for how the RFID System will be implemented and maintained in the context of the larger enterprise.” (*Id.* ¶ 16.) SAG accessed this proprietary information, among other ways, through the technical manuals GlobeRanger delivered with the Navy Solution. On the front cover, GlobeRanger warned readers:

This document contains material that is proprietary property of and confidential to GlobeRanger and its suppliers. Disclosure outside of GlobeRanger and its suppliers is prohibited except by written permission, license agreement, product evaluation license agreement or other confidentiality agreement.

(Def.’s App. 341.)

Third, GlobeRanger points to one final source in which SAG gained access to its trade secrets: Jason Miller, a former GlobeRanger employee who in late 2009 joined XIO Strategies, a contractor that worked in a support position for the RAVE team. (Pl.’s App. 421.) Like all GlobeRanger employees, Miller signed an NDA when he was hired and an exit certification when he left GlobeRanger in June 2009. (*Id.* at 97–100.) Nonetheless, Miller responded to SAG’s multiple

requests for information regarding the GlobeRanger Solution. (*See id.* at 295–99, 331–32, 396–400.) These correspondences show Miller explaining various aspects of GlobeRanger’s RFID technology, including workflows, the positioning and configuration of various components, and how GlobeRanger integrates its technology with certain computer operating systems. (*See id.*)

Despite not having an RFID solution of its own before the RAVE project, SAG now markets a product called “webMethods RFID.” (*Id.* at 330.) GlobeRanger maintains that this product “includes GlobeRanger capabilities that SAG accessed as a result of its theft of GlobeRanger’s trade secrets.” (Pl.’s Resp. 13.)

E. Resolution of the Motions to Dismiss and Remand

This case arrived in this Court on March 1, 2011, via a Notice of Removal (doc. 1). Shortly thereafter, Defendants moved to dismiss (docs. 6, 12) pursuant to Federal Rule of Civil Procedure 12(b)(6), arguing primarily that GlobeRanger’s state law claims failed as a matter of law because they were preempted by the Copyright Act. In response, GlobeRanger asserted that its claims were not preempted by the Copyright Act, and also filed a Motion to Remand (doc. 10), contending that this Court lacked subject matter jurisdiction to hear its state law claims. Though these issues have not been raised anew in the pending motion, how they were resolved is significant to the judicial estoppel/admission argument analyzed below.

In August 2011, the Court issued two memorandum opinions, both turning on its conclusion that GlobeRanger’s claims were preempted by the Copyright Act. In its first Order (doc. 27), the Court denied GlobeRanger’s Motion to Remand and found that it had jurisdiction over GlobeRanger’s claims through the Copyright Act provisions asserted by Defendants. In its second Order (doc. 28), the Court granted Defendants’ motions to dismiss and concluded, similarly, that

GlobeRanger's claims were preempted by the Copyright Act and therefore failed as a matter of law. The Court allowed GlobeRanger to replead its claims pursuant to the Copyright Act, which GlobeRanger declined to do (doc. 31), instead opting to appeal the Court's rulings.

On August 17, 2012, the Fifth Circuit reversed this Court's Rule 12(b)(6) dismissal of GlobeRanger's claims and remanded the case back to this Court for further proceedings. See *GlobeRanger Corp. v. Software AG*, 691 F.3d 702 (5th Cir. 2012). In doing so, the Fifth Circuit concluded: (1) "GlobeRanger has pled factual allegations that at least in part fall outside the scope of copyright" and are therefore not preempted, and (2) "the defendants have argued enough for a basis for preemption on GlobeRanger's conversion claim to stay in federal court." *Id.* at 710.

F. Pending Motions for Summary Judgment

Following the Fifth Circuit's remand, GlobeRanger filed the version of its complaint currently before the Court—the First Amended Complaint (doc. 79) ("FAC"). The FAC contains four Texas state law claims, including misappropriation of trade secrets, unfair competition, tortious interference with a contract, and conspiracy.

On December 18, 2013, the parties filed a Joint Motion to Continue Trial and Modify Scheduling Order (doc. 130) asking the Court, among other things, to set briefing deadlines for Defendants' anticipated "motion for summary judgment limited to the government contracts/intellectual property issue." The parties requested that the Court "consider this discrete summary judgment issue on an expedited basis."

After the Court granted the Joint Motion (doc. 131), SAG filed its Motion for Summary Judgment on January 15, 2014. Naniq joined SAG's Motion, claiming "the grounds, arguments and authorities asserted by SAG against GlobeRanger are sufficient to allow the Court to also grant

summary judgment for Naniq.” (Naniq’s Mot. Summ. J., Doc. 138.) After GlobeRanger responded to both motions, SAG filed its Reply on March 4, 2014, rendering the motions ripe for consideration.

II.

LEGAL STANDARDS

Federal Rule of Civil Procedure 56(a) provides that summary judgment is appropriate “if the movant show that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” FED. R. CIV. P. 56(a). “A fact is material if it ‘might affect the outcome of the suit under the governing law,’ and a dispute is genuine if ‘the evidence is such that a reasonable jury could return a verdict for the nonmoving party.’” *Tagore v. United States*, 735 F.3d 324 (5th Cir. 2013) (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)). In determining whether a genuine dispute exists, the Court must “consider all facts and evidence in the light most favorable to the nonmoving party [,] . . . draw all reasonable inferences in favor of the nonmoving party [,] . . . [and] disregard all evidence favorable to the moving party that the jury is not required to believe.” *Haverda v. Hay County*, 723 F.3d 586, 591 (5th Cir. 2013) (quotation marks and internal citations omitted).

Procedurally, the movant “bears the initial responsibility of informing the district court of the basis of its motion, and identifying those portions of” the record “which it believes demonstrate the absence of a genuine issue of material fact.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). Where the non-movant bears the burden of proving the material facts at trial, the movant may satisfy its summary judgment burden by “merely demonstrat[ing] an absence of evidentiary support in the record for the non-movant’s case.” *Wesley v. Gen. Drivers, Warehousemen & Helpers Local 745*, 660 F.3d 211, 213 (5th Cir. 2011) (quoting *Bayle v. Allstate Ins. Co.*, 615 F.3d 350, 355 (5th Cir.

2010)). If the movant satisfies this burden, “the burden shifts to the non–movant to produce evidence of the existence” of a genuine dispute of a material fact for trial. *Bayle*, 615 F.3d at 355.

III.

ANALYSIS

SAG moves for summary judgment on all four of GlobeRanger’s Texas state law claims, which include trade secret misappropriation, tortious interference with an existing contract, unfair competition, and conspiracy. SAG focuses primarily on the merits of GlobeRanger’s trade secret misappropriation claim. It also argues that GlobeRanger cannot establish certain essential elements of the tortious interference claim. Lastly, SAG challenges GlobeRanger’s unfair competition and conspiracy claims by arguing simply that summary judgment is appropriate for the same reasons it is proper for GlobeRanger’s other two claims. The Court addresses each disputed claim in turn.

A. *Trade Secret Misappropriation*

To establish SAG’s liability for trade secret misappropriation under Texas law, GlobeRanger must prove: “(a) a trade secret existed; (b) the trade secret was acquired through a breach of a confidential relationship or discovered by improper means; and (c) use of the trade secret without authorization.” *Wellogix, Inc. v. Accenture, L.L.P.*, 716 F.3d 867, 874 (5th Cir. 2013) (quoting *Phillips v. Frey*, 20 F.3d 623, 627 (5th Cir. 1994)). The first two elements are at issue here.¹⁴

SAG challenges the first two elements of GlobeRanger’s claim with essentially the same argument. To summarize, SAG argues that the Navy had the right to disclose all relevant technology

¹⁴ As GlobeRanger points out, SAG, in one of its footnotes, appears to address the third element as well. (See Def.’s Mot. 34 n.21.) But since SAG never explicitly cites the third element as a ground for summary judgment, the Court finds it unnecessary to consider the evidence and arguments GlobeRanger with respect to the third element.

and information surrounding the Navy Solution under governing provisions of the Defense Federal Acquisition Regulation Supplement (“DFARS”), and thus, the Court should conclude as a matter of law that (a) GlobeRanger failed to adequately protect its “secrets” and (b) SAG’s acquisition of GlobeRanger’s purported secrets, via the Navy, was lawful. But while SAG frames this dispute as purely legal—one “involv[ing] the interpretation of contracts and government regulations” (Def.’s Reply 2)—there are numerous unresolved factual issues surrounding this claim. These unresolved factual issues take shape as the Court begins its discussion of the parties’ key legal dispute—the Navy’s right to disclose the Navy Solution under DFARS—before turning to the actual trade secret elements at issue.

1. What Rights to the Navy Solution did the Navy Acquire under DFARS?

The parties take opposing positions regarding the Navy’s rights to GlobeRanger’s proprietary information under DFARS. SAG maintains that DFARS’s “technical data” or “noncommercial computer software” provisions apply, and as such, the Navy indisputably had the right to disclose GlobeRanger’s technology and information. GlobeRanger, on the other hand, argues that DFARS’s “commercial computer software” provisions apply, and therefore, the Navy did not have the right to disclose the Navy Solution in these circumstances.

i. Legal issues surrounding the Navy’s rights under DFARS

In general, all government contracts are subject to the Federal Acquisition Regulations (“FAR”). For DoD contracts, FAR is supplemented by DFARS, whose technology provisions regulate the Navy contracts relevant to this dispute.¹⁵ The DFARS provisions at issue are most easily

¹⁵ Citations made herein are to the version of FARS and DFARS in effect in December 2007, when the subcontract between GlobeRanger and SAIC was signed. That said, the DFARS provisions

addressed by posing two related questions: (1) which set of DFARS provisions govern? and (2) what disclosure rights do these governing regulations grant the Navy under the circumstances of this case?

First, the Court asks whether DFARS's technical data, noncommercial computer software, or commercial computer software regulations apply. This issue seems to turn on whether the contractual item at issue qualifies as "technical data," "noncommercial computer software," or "commercial computer software/commercial computer software documentation."

DFARS 252.227-7013 covers the government's "Rights in Technical Data—Noncommercial Items." Technical data refers to "recorded information, regardless of the form or method of the recording, of a scientific or technical nature." 48 C.F.R. § 252.227-7013(a)(14). Notably, technical data "does not include computer software." *Id.* And for all practical purposes, "computer software documentation" is also excluded from the technical data regulations.¹⁶

DFARS 252.227-7014 regulates the government's "Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation." Computer software is defined as "computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled." *Id.* § 252.227-7014(a)(4). Computer software

central to this case have not been significantly altered since 1995. See Peter Dugan, *Less is More: Encouraging Greater Competition in Computer Software Procurement by Simplifying the DFARS Licensing Scheme*, 39 Pub. Cont. L.J. 465, 469 (2010).

¹⁶ Technical data's definition actually encompasses "computer software documentation." 48 C.F.R. § 252.227-7013(a)(14). But confusingly, the technical data regulations elsewhere indicate that the government's technical data rights do not apply to computer software documentation. See *id.* § 252.227-7013(b). Instead, computer software documentation is governed either the noncommercial or commercial computer software regulations, depending on what type of software the documentation relates to.

documentation under DFARS “means owner’s manuals, user’s manuals, installation instructions, operation instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.” *Id.* § 252.227–7014(a)(5). Computer software and its documentation are “noncommercial” so long as the computer software does *not* fit the definition of “commercial computer software.” *Id.* § 252.227–7014(a)(13).

DFARS § 227.7202 governs the DoD’s rights in “Commercial Computer Software” and “Commercial Computer Software Documentation.” Computer software and its documentation are “commercial” if the computer software qualifies as “commercial computer software” under DFARS’s definition, which covers “software developed or regularly used for non-governmental purposes” that meet one of the following four criterion:

- (i) Has been sold, leased, or licensed to the public;
- (ii) Has been offered for sale, lease, or license to the public;
- (iii) Has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this contract; or
- (iv) Satisfies criterion expressed in paragraph (a)(1)(i), (ii), or (iii) of this clause and would require only minor modification to meet the requirements of this contract.

Id. § 252.227–7014(a)(1). The Navy Solution can only qualify as “commercial computer software” if it meets criterion (iv) listed above—the “minor modification” criterion—because, as GlobeRanger concedes, the Navy Solution is not an out-of-the-box product. A “minor modification” is one “that does not significantly alter the non-governmental function or purpose of the software or is of the type customarily provided in the commercial marketplace.” *Id.* § 252.227-7014(a)(12).

Second, after determining which set of DFARS regulations apply, the next question to

consider is what rights the applicable regulations grant the Navy in these circumstances. More specifically, what *disclosure* rights could the Navy have acquired under each set of regulations? As detailed below, the undisputed facts show that the Navy's disclosure was permissible under DFARS if the technical data or noncommercial software regulations apply, but if the commercial software regulations apply, the Navy's disclosure would not have been undisputedly permitted by DFARS.

Pursuant to DFARS § 252.7013's provisions, the government may obtain one of three licenses in technical data. *Id.* § 252.227–7013(b). The broadest technical data license—“unlimited rights”—grants the government the right, among other things, to “disclose technical data in whole or in part, in any manner, and for any purposes whatsoever, and to have or authorize others to do so.” *Id.* § 252.227–7013(a)(15). The second tier license—“government purpose rights”—also allows the government to disclose the technical data, but not “for commercial purposes.” *Id.* § 252.227–7013(a)(12). The third is the “limited rights” license, which prohibits unauthorized disclosures of technical data. *Id.* § 252.227–7013(a)(13). Which of the three technical data licenses the government obtains depends on various factors, only one of which requires discussion for purposes of this motion.¹⁷ Specifically, unless the technical data is “conspicuously” marked in accordance with the regulation's strict requirements detailed in DFARS § 252.277–7013, the government, by default, obtains an unlimited rights license to the unmarked technical data. *Id.* § 252.227–7013(f). Here, since GlobeRanger never claims it marked the Navy Solution in accordance with DFARS § 252.277–7013, the Navy indisputably obtained an unlimited rights license if GlobeRanger delivered technical data. Thus, if the Navy Solution or its relevant components qualify

¹⁷ A second, potentially relevant, factor is the source of funding (i.e., government or private) for the technical data's development. But the Court need not address this factor for purposes of this motion.

as technical data, the Court must conclude, as a matter of law, that the Navy had the right to disclose this technical data to SAG.

Under DFARS § 252.7014's noncommercial software regulations, the Court would be compelled to reach the same conclusion as it would under DFARS's technical data regulations. As GlobeRanger admits, the noncommercial software regulations are “just like [the] technical data” regulations in that both “provide the government with different types of rights depending on factors such as . . . the use of restrictive legends.” (Pl.’s Resp. 24.) Therefore, the Court must, likewise, conclude that the Navy indisputably had the right to disclose the Navy Solution and its components if they qualify as noncommercial software or noncommercial software documentation.

DFARS § 227.7202's commercial software regulations are more favorable to DoD contractors. These provisions provide that “[c]ommercial computer software and commercial computer software documentation shall be acquired under the licenses customarily provided to the public unless such licenses are inconsistent with Federal procurement law or do not otherwise satisfy user needs.” *Id.* § 227.7202–1(a). Thus, if the Navy Solution and its components qualify as “commercial computer software” or “commercial computer software documentation,” no default government licenses attach to GlobeRanger’s proprietary information. Instead, DFARS instructs that these commercial items “shall be acquired under the licenses [GlobeRanger] customarily provided to the public,” which—if agreed to by the Navy—would be GlobeRanger’s EULA.

To summarize, the Navy’s disclosure rights primarily turn on how the Navy Solution and its components are characterized under DFARS’s technology provisions. Favoring SAG, if the Navy Solution and its relevant components qualify, as a matter of law, as “technical data,” “noncommercial computer software,” or “noncommercial computer software documentation,” the undisputed facts

show that the Navy's disclosure of GlobeRanger's proprietary information to SAG was permissible under DFARS. Favoring GlobeRanger, if the Navy Solution or its relevant components reasonably qualify as "commercial computer software" or "commercial computer software documentation," the default license rights in DFARS's technical data and noncommercial software provisions do not apply, and as such, the Navy's disclosure would not have been undisputedly permitted by DFARS.

ii. *Genuine disputes exist regarding the Navy's rights under DFARS*

While the above discussion appears to present a pure legal dispute, the summary judgment record reveals a number of genuine factual issues that confound the Court's attempt to discern the Navy's precise rights under DFARS. The primary disputes, as follows, are whether the Navy Solution and its relevant components qualify as (1) "technical data" or "computer software," and (2) whether the software components fall under the "commercial computer software" definition.

First, a genuine dispute exists as to whether the Navy Solution qualifies as "computer software" under DFARS. The summary judgment record shows the Navy Solution to be made up of hardware, software, and other components, all of which GlobeRanger added its know-how and experience to during the implementation process. Because of this mixture, SAG—who concedes that at least part of the Navy Solution contained software¹⁸—attempts to break the Solution down into discrete components and show that the Navy had the right to disclose each relevant component under DFARS. The relevant components identified by SAG include "[t]he data that [SAG] allegedly sought to replicate (GlobeRanger's Architecture and Business Processes) and the items that [SAG]

¹⁸ SAG does not dispute that the Navy Solution consists, at least in part, of "computer software" as defined by DFARS. (See Def.'s Mot. 3.)

allegedly acquired to facilitate the misappropriation of trade secrets (the license keys . . .)¹⁹,” which “are all technical data” according to SAG. (Def.’s Mot. 14.) But there are two major shortcomings in SAG’s suggested approach.

The first is that GlobeRanger’s theory of liability, and supporting evidence, require a more holistic view of SAG’s theft, which trade secret misappropriation law allows. GlobeRanger contends, and the evidence reasonably suggests, that SAG unlawfully accessed the entire Navy Solution and used it to reverse-engineer its own RFID solution with webMethods as a base. This holistic approach is sufficient under the flexible legal standards governing trade secret misappropriation,²⁰ even though the summary judgment record does not clearly indicate which particular Navy Solution components SAG “acquired” or “used.” But the Navy Solution’s mixture of relevant components leaves the Navy’s rights to the entire Solution unclear under the rigid definitions of DFARS, which—in contrast to trade secret law—purports to clearly delineate the parties’ rights to tangible items delivered pursuant to DoD contracts. Nonetheless, as mentioned, GlobeRanger’s burden here is merely to show that genuine factual issues exist regarding the lawfulness of the Navy’s disclosure.

¹⁹ SAG also discusses GlobeRanger’s partial data dictionary, but as mentioned above in the Background section, GlobeRanger does not press this as a source of its trade secrets.

²⁰ See, e.g., *Metallurgical Indus. Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1201-02 (5th Cir. 1986) (“Because each case must turn on its own facts, no standard formula for [determining whether a trade secret exists] can be devised. . . . The definition of “trade secret” will therefore be determined by weighing all equitable considerations.”); *Lamont v. Vaquillas Energy Lopeno Ltd.*, 421 S.W.3d 198, 213 (Tex. App. 2013) (“A complete catalogue of improper means [for purposes of the second trade secret element] is not possible. In general they are means which fall below the generally accepted standards of commercial morality and reasonable conduct.”) (quotations and citations omitted); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1995) (“There are no technical limitations on the nature of the conduct that constitutes ‘use’ of a trade secret As a general matter, any exploitation of the trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant is a ‘use’ [for purposes of trade secret liability].”).

And since GlobeRanger has shown that at least part of what the Navy disclosed qualifies as “computer software,” the Court cannot agree with SAG that the Navy’s disclosure was indisputably lawful under DFARS’s “technical data” provisions.

The second problem with SAG’s proposed analysis has to do with its argument regarding the classification of the Navy Solution components identified in GlobeRanger’s FAC. Contrary to SAG’s contentions, the evidence does not undisputedly show that the Navy had the right to disclose these items, which include GlobeRanger’s Architecture, Business Processes, and license keys.

For GlobeRanger’s Architecture and Business Processes, genuine factual issues exist regarding whether these items are “technical data” or “computer software.” Under DFARS, only “recorded information” qualifies as “technical data.” 48 C.F.R. § 252.227–7013(a)(14). To show GlobeRanger’s Architecture and Business Processes are “recorded information,” SAG cites, without explanation, GlobeRanger’s technical manuals that were delivered with the Navy Solution. (Def.’s Mot. 14 nn. 13, 14.) While this arguably suggests that GlobeRanger’s Architecture and Business Processes were recorded in some form, other evidence depicts these items as nothing more than abstract concepts emanating from the Navy Solution’s various components. In relation to the Architecture, for example, GlobeRanger’s employees have described a “design process” by which GlobeRanger arranges its RFID technology using its experience and know-how, deciding, for instance, which expansion packs to use or how many device adapters to install in light of the RFID-reader layout. (Pl.’s App. 338–39.) Similarly, evidence suggests that the Business Processes are standard ideas and methods that GlobeRanger developed over time to turn simple tag reads into useful business events. (See, e.g., FAC ¶ 15.) These abstract concepts may have been brought to life through the Navy Solution’s tangible components, but that does not mean these ideas and processes were thereby deemed

“recorded” and delivered as “technical data” to the Navy. Indeed, a reasonable juror could just as well conclude that GlobeRanger’s Architecture and Business Processes qualify as “computer software” in light of the evidence showing that these concepts originate from the Navy Solution’s tangible components, which include computer software.

To the extent the Business Processes and Architecture are “recorded” in GlobeRanger’s technical manuals, as SAG contends, the evidence reasonably shows this item to be “commercial computer software documentation” under DFARS. As mentioned, computer software documentation includes “owner’s manuals, user’s manuals, installation instructions, operating instructions, and other similar items . . . that explain the capabilities of the computer software or provide instructions for using the software.” 48 C.F.R. § 252.227–7013(a)(4). Here, the evidence reasonably shows that the technical manuals contain installation and operating instructions explaining the capabilities and use of the Navy Solution’s software, qualifying the manuals as “computer software documentation.” (See Def.’s App. 340–67.) The evidence also demonstrates that the manuals were “commercial” because they relate to the Navy Solution’s software, which, as discussed below, reasonably comports with the “commercial computer software” definition.

Likewise, a genuine dispute exists regarding whether GlobeRanger’s license keys qualify as “technical data” or “computer software.” GlobeRanger submits evidence describing the license key as “a special security *program* . . . owned and operated by GlobeRanger [that] may be required to render operational the Licensed Software.” (Pl.’s App. 86 (emphasis added).) The evidence also shows that the license key is a device specific and node-locked, meaning that GlobeRanger’s software cannot be accessed for the first time or on any new device without the license key activating the software. (*Id.* at 426.) This is enough to allow a reasonable juror to conclude that GlobeRanger’s

license keys qualify, under DFARS's "computer software" definition, as a "computer progra[m]" or some sort of "related material that would enable the software to be reproduced, recreated, or recompiled." 48 C.F.R. § 252.227-7014(a)(4).

Second, having found the evidence reasonably shows that the Navy Solution's relevant components qualify as "computer software," the Court similarly concludes that a genuine dispute exists regarding whether this software is "commercial." Under the circumstances of this case, the definition of "commercial computer software," cited in full above, can be broken down into three requirements that GlobeRanger must establish. Specifically, the Navy Solution's software must: (1) have been "developed or regularly used for non-governmental purposes," (2) "[s]atisf[y] criterion expressed in paragraph (a)(1)(i), (ii), or (iii) of" the commercial software definition,²¹ and (3) "require only minor modification to meet the requirements of [the Navy] contract." 48 C.F.R. § 252.227-7014(a)(1).

Here, genuine disputes exist for each of the above three requirements. For the first, GlobeRanger shows that the Navy Solution's core, software-related components—the iMotion platform, Solution Accelerators, and Expansion Packs—are "regularly used" in the GlobeRanger Solution package licensed to non-governmental customers. (See Pl.'s App. 1-24, 414-16.) While SAG contends otherwise, its argument raises factual issues requiring credibility choices that are not for the Court to resolve at this point in the proceedings. Likewise, the second requirement is met,

²¹ See 48 C.F.R. § 252.227-7014(a)(1) (providing that commercial software "(i) Has been sold, leased, or licensed to the public; (ii) Has been offered for sale, lease, or license to the public; (iii) Has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this contract; or (iv) Satisfies criterion expressed in paragraph (a)(1)(i), (ii), or (iii) of this clause and would require only minor modification to meet the requirements of this contract").

because the evidence shows, for the same reasons just discussed, that the Navy Solution's software "has been sold, leased, or licensed to the public" as required by paragraph (a)(1)(i) of the commercial software definition. The bigger question here, is whether GlobeRanger's modifications to its GlobeRanger Solution in building the Navy Solution qualify as "minor" under DFARS.

As a reminder, a "minor modification" is one "that does not significantly alter the nongovernmental function or purpose of the software or is of the type customarily provided in the commercial marketplace." *Id.* § 252.227-7014(a)(12). Here, there is a genuine factual dispute regarding whether the Navy Solution's modifications are those "customarily provided" to GlobeRanger's commercial customers. GlobeRanger's representatives aver that the Navy Solution's customizations are "minor" in that GlobeRanger "customarily provide[s]" these same type of modifications in a commercial setting. (Pl.'s App. 337-39, 417-18.) This includes, for example, modifying the GlobeRanger Solution's workflows to integrate with Navy's Oracle database in the same way GlobeRanger modifies workflows for its commercial customers who also employ an Oracle database. (*Id.* at 418.) Similarly, another GlobeRanger representative's testimony shows that GlobeRanger altered the GlobeRanger Solution's Expansion packs to meet the Navy's needs in the same soft of way GlobeRanger "customarily" does for commercial customers. (*See id.* at 338.) Though a jury may ultimately find these modifications to be more than "minor" as defined by DFARS, GlobeRanger has presented enough evidence, at this point, for a reasonable juror to conclude that the Navy Solution contains "commercial computer software" under DFARS.

In sum, the Court concludes that genuine issues of fact exist regarding whether the Navy Solution qualifies as technical data, noncommercial computer software, or commercial computer software under DFARS. As such, the Court cannot conclude, as a matter of law, that the Navy had

the right to disclose the Navy Solution under DFARS “technical data” or “noncommercial computer software” regulations. And based on the Court’s above discussion regarding the Navy’s rights to commercial computer software, as well as the below analysis that expands on this discussion, the Court cannot conclude as a matter of law that the Navy had the right to disclose the Navy Solution, which the evidence reasonably shows to be made up, at least in part, of commercial computer software.

iii. Addressing SAG’s counter-arguments

In its Reply, SAG emphasizes three points that it believes show that the Navy’s disclosures were indisputably lawful despite the genuine factual issues just discussed. These counter-points include: (a) GlobeRanger is foreclosed from arguing that its RFID solution is “computer software” in light of its prior representations in this case, (b) the written government contracts in this case did not call for commercial software, and as such, GlobeRanger cannot establish that the commercial software regulations govern, and (c) since the government at least partially funded the Navy Solution, GlobeRanger cannot show that its software was commercial. (Def.’s Reply 5.) As explained below, none of these argument persuade the Court to conclude, as a matter of law, that the Navy was permitted to disclose GlobeRanger’s RFID technology under DFARS.

a. Judicial admission/estoppel

SAG’s first contention is that the doctrines of judicial estoppel and admission foreclose GlobeRanger’s “commercial computer software” arguments in light of its prior statements concerning preemption under the Copyright Act. Specifically, SAG highlight GlobeRanger’s representations in its Fifth Circuit Appellate Brief that: the “Complaint defines the GlobeRanger RFID Solution as something markedly different” than “computer software,” as it is defined by the Copyright Act; the

allegations specifically state “that Defendants did not copy GlobeRanger’s software”; and the alleged trade secrets involve “elements external to the [computer] program, such as GlobeRanger’s Business Processes and Architecture.” (Def.’s Reply (quoting Def.’s App. 1, 4, 8) (emphasis omitted).) As SAG points out, the Fifth Circuit ultimately sided with GlobeRanger on the copyright preemption issue, reasoning that “[e]ven though the allegations . . . include copying of specific expressions” of computer software, GlobeRanger also “alleges that it implements RFID solutions” that “include the types of procedures, processes, systems, and method of operation that are excluded from copyright protection under” the Copyright Act.²² *GlobeRanger Corp.*, 691 F.3d at 708–09.

Based on the foregoing, SAG maintains that the “Court should treat GlobeRanger’s [prior] statements . . . as judicial admissions or judicial estoppel” and prohibit GlobeRanger from arguing that the Navy Solution qualifies as “computer software” under DFARS. (Def.’s Reply 7.) GlobeRanger counters that it is not foreclosed from making this argument, because its prior position was simply “that this case is not about *literal copying of software*.” (Pl.’s Resp. 19 (emphasis in original).) Instead, according to GlobeRanger, its “core allegations has always been . . . that SAG wrongfully obtained a live, customized configuration of GlobeRanger Solution, and then spent months in a secret lab, accessing, studying, and reverse engineering *how* the GlobeRanger Solution worked and achieved its various functionalities.” (*Id.* at 20 (emphasis in original).) Since it agrees that GlobeRanger’s positions are not inconsistent, the Court finds that GlobeRanger is not foreclosed

²² For the copyright preemption defense to apply, a two prong test must be satisfied. GlobeRanger’s above-cited representations relate to the first prong: whether the claim falls within the subject matter of the Copyright Act, which excludes from protection “any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.” 17 U.S.C. § 102(b).

from arguing that the Navy Solution is “computer software.”

First, judicial estoppel does not foreclose GlobeRanger’s “computer software” arguments. According to the Fifth Circuit, “[j]udicial estoppel is a common law doctrine that prevents a party from assuming inconsistent positions in litigation.” *In re Superior Crewboats, Inc.*, 374 F.3d 330, 334 (5th Cir. 2004). As “courts have uniformly recognized,” judicial estoppel’s “purpose is to protect the integrity of the judicial process by prohibiting parties from deliberately changing positions according to the exigencies of the moment.” *New Hampshire v. Maine*, 532 U.S. 742, 749 (2001) (internal citations and quotation marks omitted). The Fifth Circuit has “‘identified at least two limitations on the application of the doctrine: (1) it may be applied only where the position of the party to be estopped is clearly inconsistent with its previous one; and (2) that party must have convinced the court to accept that previous position.’” *Ahrens v. Perot Sys. Corp.*, 205 F.3d 831, 833 (5th Cir. 2000) (quoting *In re Coastal Plains, Inc.*, 179 F.3d 197, 205 (5th Cir. 1999)). Nonetheless, since “judicial estoppel is an equitable doctrine, [] the decision whether to invoke it [is] within the [district] court’s discretion.” *Coastal Plains*, 179 F.3d at 205.

Here, judicial estoppel is not applicable because GlobeRanger has not “asserted a legal position that is ‘plainly inconsistent’ with a position asserted in a prior case.” *In re Oparaji*, 698 F.3d 231, 235 (5th Cir. 2012) (*Love v. Tyson Foods, Inc.*, 677 F.3d 258, 261 (5th Cir.2012)). In relation to copyright preemption, GlobeRanger *emphasized* the non–software components of the Navy Solution in an effort to show that its allegations do not involve the copying of computer software’s expressive elements. Now, GlobeRanger *emphasizes* the software components of the Navy Solution in an effort to establish a completely different legal proposition—that the Navy did not have the right to disclose the Navy Solution to SAG. In both instances, GlobeRanger’s “core allegations” are the

same: “SAG wrongfully obtained a live, customized configuration of GlobeRanger Solution”—whose software components are emphasized in this motion—“and then spent months in a secret lab, accessing, studying, and reverse engineering” the Solution’s non-expressive elements, namely, “*how* [it] worked and achieved its various functionalities.” (Pl.’s Resp. 20 (emphasis in original).)

To the extent GlobeRanger’s legal positions are inconsistent at all, that inconsistency is implied. But the Fifth Circuit has “expressed reluctance to apply judicial estoppel in situations where a party’s alleged change of position is merely implied rather than clear and express.” *Oparaji*, 698 F.3d at 237. Without question, GlobeRanger, in emphasizing the non-expressive elements of its RFID technology for purposes of preemption, did not “clearly” or “expressly” adopt a different position than the one it takes now regarding the characterization of the Navy Solution under DFARS. Indeed, “[d]espite the semantic inconsistency, it is legally possible” for GlobeRanger to adopt these two positions regarding the role of software in this case and still prevail on both grounds.²³ *Hopkins v. Cornerstone Am.*, 545 F.3d 338, 347 (5th Cir. 2008). Accordingly, given that there is no “legal inconsistency” in its positions, GlobeRanger cannot be estopped from arguing that its RFID solution contains “computer software” as defined by DFARS. *Id.*

Second, GlobeRanger is also not foreclosed from arguing that the Navy Solution qualifies as computer software under the doctrine of judicial admissions. As the Fifth Circuit notes, “[a] judicial admission is a formal concession in the pleadings or stipulations by a party or counsel that is binding

²³ Compare *GlobeRanger*, 691 F.3d at 707 (explaining that while “nonliteral aspect of computer programs are within the scope of copyright [,] . . . copyright protection [does not] swee[p] so broadly as to encompass whole structures or systems of which software is only a part”), *with* 48 C.F.R. § 252.227–7013(a)(3) (defining computer software broadly to encompass even “processes, flow charts, formulae and related material that would enable the software to be reproduced, recreated, or recompiled”).

on the party making them.” *Martinez v. Bally's Louisiana, Inc.*, 244 F.3d 474, 476 (5th Cir. 2001). Whereas judicial estoppel deals with a party’s positions on a legal issue, judicial admission concerns a party’s factual representations. When applicable, a judicial admission “has the effect of withdrawing a fact from contention.” *Id.* For the doctrine to apply, the purported admission “must be made intentionally as a waiver, releasing the opponent from proof of fact.” *United States v. Chavez–Hernandez*, 671 F.3d 494, 501 (5th Cir. 2012) (quoting *Martinez*, 244 F.3d at 476). And like judicial estoppel, the doctrine of judicial admissions cannot be used to exclude a party’s present statement unless it is “inconsistent with or contrary to” its past statement. *Giddens v. Cmty. Educ. Centers, Inc.*, 540 F. App’x 381, 390-91 (5th Cir. 2013) (citing *Davis v. A.G. Edwards & Sons, Inc.*, 823 F.2d 105, 107–08 (5th Cir.1987)). As before, whether to treat prior “statements in briefs as binding judicial admissions of fact . . . is within [the Court’s] discretion.” *City Nat. Bank v. United States*, 907 F.2d 536, 544 (5th Cir. 1990).

As with judicial estoppel, the Court concludes that the doctrine of judicial admissions does not apply, since GlobeRanger’s prior statements are not “contrary to a fact essential to the theory of recovery.” *Heritage Bank v. Redcom Labs., Inc.*, 250 F.3d 319, 329 (5th Cir. 2001). GlobeRanger never claimed, while arguing preemption, that its RFID technology does not include computer software or that the Navy had the right to any of its technology at issue under DFARS. And as detailed above, its prior statements are consistent with its current representation; GlobeRanger has simply emphasized different aspects of the RFID technology while arguing two completely different legal issues. Even assuming GlobeRanger’s representations contain factual inconsistencies, there is no reasonable indication that GlobeRanger made its prior statements “intentionally as a waiver, releasing [SAG] from proof of fact” regarding the Navy Solution’s composition or the Navy’s rights

to GlobeRanger's technology. *Martinez*, 244 F.3d at 476. Accordingly, the Court has no reasonable basis to exclude GlobeRanger's "computer software" representations under the doctrine of judicial admissions.

Lastly, GlobeRanger's arguments concerning the Navy Solution's "commercial" nature are, likewise, not foreclosed under the doctrines of judicial estoppel or admissions. SAG highlights a second set of representations by GlobeRanger that it believes are inconsistent. Specifically, SAG points out that GlobeRanger previously argued, in its Motion to Remand, that the Navy Solution was a custom-built solution, not an out-of-the-box product. (Def.'s Reply 6 (citing Def.'s App. 430-31).). SAG claims that these prior representations should foreclose GlobeRanger from arguing now that the Navy Solution contains GlobeRanger's "existing, commercially-available platform and component capabilities" with "minor modification[s]," as defined by the DFARS's "commercial computer software" regulations. (*Id.* (citing Pl.'s Resp. 9).) But like before, these prior statements are neither legally nor factually inconsistent with GlobeRanger's representations. In its current brief, GlobeRanger even admits "every solution [it] sells is slightly different"; it simply goes on to elaborate, as it did not do in its Motion to Remand brief, that these differences constitute "minor modification[s]" under DFARS. (Pl.'s Resp. 25.) These representations simply supplement the prior representations—there is no inconsistency. And even if there was, the Court cannot foreclose GlobeRanger's arguments for additional reasons. For judicial estoppel, the Court did not rely on GlobeRanger's representations when it denied GlobeRanger's Motion to Remand. For judicial admission, there is no indication that GlobeRanger's prior representations were intended to release SAG from proof of fact regarding the degree to which the Navy Solution was modified. Accordingly, neither judicial estoppel nor judicial admission apply in these circumstances.

b. The lack of a written commercial software contract

The next point SAG raises is that “the prime contract and subcontract that undisputedly governed GlobeRanger’s work for the Navy call for GlobeRanger to provide services and technical data,” and “[t]here is no evidence that GlobeRanger ever entered into any licensing agreement or contract to provide commercial computer software to the Navy.” (Def.’s Reply 5.) According to SAG, since the evidence shows that GlobeRanger failed “to push SAIC to obtain [a commercial software] licensing arrangement from the Navy[,] . . . it must live with the contracts that govern its work for the Navy, which involve technical data and not commercial software.” (*Id.* at 12.)

The only real counter GlobeRanger seems to offer is that, as long as the Navy Solution contained “commercial computer software” as defined by DFARS, the regulations *automatically* bind the Navy to GlobeRanger’s EULA, even if no evidence shows the Navy actually agreed to be bound by the EULA’s terms. But as discussed in relation to GlobeRanger’s tortious interference claim, DFARS does not seem to support this argument made by GlobeRanger. Nonetheless, this deficiency does not prevent the Court from finding in GlobeRanger’s favor for its trade secret claim.

To be fair, DFARS leaves the Navy’s rights somewhat uncertain in these circumstances—where a subcontractor delivers commercial computer software to the government without indicating in its written subcontract or in any direct agreement with the government that commercial software is involved. But this legal ambiguity regarding the parties’ contractual rights does not mean the Court must adopt SAG’s position for purposes of GlobeRanger’s trade secret claim. In fact, the main problem with SAG’s argument is that it seemingly forgets that GlobeRanger is not obligated, under trade secret misappropriation law, to show that the Navy’s rights were

restricted by the EULA or some other written or even express agreement.²⁴ Instead, GlobeRanger simply must show, at least for this portion of the analysis, that genuine factual disputes exist in regard to the Navy's right to disclose the Navy Solution. As detailed above, GlobeRanger has done just that. What SAG now points to is merely evidence (written contracts) supporting its own factual position that GlobeRanger delivered technical data and/or noncommercial software, rather than commercial software. What SAG fails to identify, however, is some legal authority that would persuade the Court to find that the Navy, by default, obtains the right to disclose a subcontractor's commercial software simply because the subcontractor did not procure the Navy's express acceptance of the commercial license's terms.

For starters, DFARS's commercial software regulations make clear that "[a] specific contract clause governing the government's rights in commercial computer software or commercial computer software documentation is not prescribed." 48 C.F.R. § 227.7202-4. This is in stark contrast to the technical data and noncommercial software provisions, which require contractors to incorporate particular clauses in their government contracts and follow specific procedures, or else the government will automatically obtain specific, default license rights in the technology in question. The commercial software regulations have no such pre-conditions before a contractor can assert its rights. And should the government and contractor fail to follow DFARS's instructions to see that the commercial software is "acquired under the license customarily provided to the public," the commercial software regulations provide no back-up, default license rights like the technical data

²⁴ See *Phillips v. Frey*, 20 F.3d 623, 631 (5th Cir. 1994) ("[T]he Supreme Court of Texas [has] held that an express agreement was not necessary [for a trade secret claim] where the actions of the parties and the nature of their relationship, taken as a whole, established the existence of a confidential relationship.").

and noncommercial software provisions. *Id.* § 227.7202–1(a).

Moreover, nothing in DFARS suggests that technology qualifying as “commercial computer software” somehow reverts to “noncommercial computer software” or “technical data” and becomes governed by those DFARS provisions simply because the parties’ rights are unclear under the commercial software regulations. In fact, the applicable set of DFARS regulations is determined solely based on whether the technology at issue qualifies as technical data (DFARS § 252.227–7013), noncommercial software (DFARS § 252.227–7014), or commercial software (DFARS § 227.7202). If the applicable regulation was, instead, determined by how the parties define the technology in their written contracts as SAG suggests, then DFARS’s detailed definitions of these applicable terms would be meaningless.

Finally, neither government contract provision cited by SAG convince the Court to find differently. First, SAG points to a regulation instructing the government and contractors not to “use the [technical data] clause when the only deliverable items are computer software or computer software documentation.” *Id.* § 227.7103–6(a). But again, the summary judgment record shows the Navy Solution contained a mixture of components, which makes it is entirely reasonable to conclude that GlobeRanger delivered both technical data and computer software, and thus, there is no violation of this provision.²⁵ Second, SAG also highlights a single sentence from the commercial software regulations stating: “The specific rights granted to the Government shall be enumerated in the contract license agreement or an addendum thereto.” *Id.* § 227.7202–3(b). But immediately

²⁵ Even if only software and software documentation was delivered, this DFARS provision is merely intended to instruct the parties on when to use the technical data provision. If, for example, the contractor and government accidentally included the technical data provision when only software was delivered, the provision, by its terms, would not automatically render the delivered items “technical data.”

preceding this isolated sentence is another that reads: “If the Government has a need for rights not conveyed under the license customarily provided to the public, the Government must negotiate with the contractor to determine if there are acceptable terms for transferring such rights.” *Id.* Thus, reading the entire clause—rather than the isolated portion SAG cites—shows that, in the event “the Government has a need for rights not conveyed” in the contractor’s commercial software license and decides to negotiate for more rights, only then must the Government’s “specific rights” to the commercial software “be enumerated in [a] contract license agreement or addendum thereto.” *Id.* Since this is clearly not the circumstances of this case—the Navy never indicated it needed greater rights and no negotiations took place—GlobeRanger was not required to enumerate the Navy’s specific rights to its commercial software in a written contract.

c. Source of funding for the commercial software

The third and final counter–argument raised by SAG is that the Navy Solution’s software “is not commercial because it was developed exclusively for the Navy using U.S. taxpayer funds.” (Def.’s Reply 13.) But the commercial software regulations, unlike the technical data and noncommercial software regulations, do not grant the government different rights based on the commercial software’s source of funding. Instead, they simply require that the software qualify as “commercial,” which includes commercial software that contains “minor modification[s],” regardless of whether those modifications were funded by the government or otherwise.²⁶ 48 C.F.R. § 252.227–7014(a)(1). Thus,

²⁶ See Andrea B. Mayner, *Understanding DFARS Technical Data Rights Regulations*, CONT. MGMT., Nov. 2004, at 16, 23 (noting that “contractors are able to make minor modifications to commercial software at government expense” under DFARS and the software “will still be considered commercial”); see also Christine C. Trend, *Killing the Goose that Laid the Golden Egg: Data Rights Law and Policy in Department of Defense Contracts*, 34 Pub. Cont. L.J. 287, 323 (2005) (noting the same).

so long as the Navy Solution qualifies as commercial computer software, it makes no difference whether the Navy paid for any portion of GlobeRanger's developmental work. And since the Court already found genuine issues exist regarding whether the Navy Solution qualifies as commercial software, the Court rejects SAG's contention that the Navy indisputably had the right to disclose the Navy Solution in light of the government funding GlobeRanger apparently received.

2. Trade Secret Misappropriation Elements in Dispute

Having found that genuine factual issues surround the Navy's right to disclose the Navy Solution, the Court now turns to the two disputed trade secret misappropriation elements in this case: (1) the existence of a trade secret, and (2) acquisition of the trade secret through a breach of confidence or improper means.

i. Element 1: Existence of a Trade Secret

Under Texas law, "[a] trade secret is 'any formula, pattern, device or compilation of information which is used in one's business and presents an opportunity to obtain an advantage over competitors who do not know or use it.'" *Southwestern Energy Prod. Co. v. Berry-Helfand*, 411 S.W.3d 581, 597 (Tex. App. 2013) (quoting *In re Bass*, 113 S.W.3d 735, 739 (Tex. 2003)). Whether a trade secret exists "is properly considered a question of fact to be decided by the judge or jury as fact-finder." *Wellogix*, 716 F.3d at 874 (quoting *Gen. Universal Sys., Inc. v. Lee*, 379 F.3d 131, 150 (5th Cir. 2004)).

SAG does not challenge GlobeRanger's ability to show that the Navy Solution contained trade secrets. Rather, SAG contends that GlobeRanger's proprietary information lost its trade-secret status when GlobeRanger delivered the Navy Solution to the Navy without adequate protections. More specifically, SAG maintains that since "GlobeRanger provided its RFID solution to the Navy

without restriction, the RFID solution does not qualify for trade secret protection.” (Def.’s Mot. 25.) But given the Court’s above conclusions regarding the Navy’s disputed rights under DFARS, SAG’s contention is without merit.

First, the primary line of authority SAG relies on here can be easily dismissed. SAG compares these circumstances to federal cases in which DoD contractors lost the trade–secret status of their “technical data” upon delivering such data to the government without complying with DFARS’s marking requirements.²⁷ But since genuine factual issues exist regarding whether the Navy Solution’s relevant components qualify as technical data, the Court finds these cases distinguishable.

Second, SAG also relies on cases applying Texas law to more generally argue that GlobeRanger’s disclosure of its RFID technology to the Navy destroyed the secrecy of its supposed trade secrets. As SAG points out, “[a] trade secret must be a secret” under Texas law.²⁸ Applying this principle, courts “have held that the unrestricted disclosure of trade–secret information to third parties, outside the context of a confidential relationship, destroys the trade–secret status of the information.”²⁹ But importantly, disclosure only defeats the information’s trade–secret status if the

²⁷ See, e.g., *L–3 Commc’ns Westwood Corp. v. Robichaux*, No. 06–279, 2008 WL 577560, at *8 (E.D. La. Feb. 29, 2008); *Secure Servs. Tech., Inc. v. Time & Soace Processing, Inc.*, 722 F. Supp. 1354, 1360 (E.D. Va. 1989); *Conax Fl. Corp. v. United States*, 824 F.2d 1124, 1128 (D.C. Cir. 1987).

²⁸ *INEOS Grp. Ltd. v. Chevron Phillips Chem. Co.*, 312 S.W.3d 843, 852 (Tex. App. 2009); see also *Luccous v. J.C. Kinley Co.*, 376 S.W.2d 336, 338 (Tex. 1964) (“It is self–evident that the subject matter of a trade secret must be kept secret.”); *Southwestern Energy Prod. Co. v. Berry–Helfand*, 411 S.W.3d 581, 597 (Tex. App. 2013) (“There must be a substantial amount of attendant secrecy for information to be a trade secret.”).

²⁹ *INEOS Grp.*, 312 S.W.3d at 852 (citing *Numed, Inc. v. McNutt*, 724 S.W.2d 432, 435 (Tex. App. 1987) and *Interlox America v. PPG Indus., Inc.*, 736 F.2d 194, 202 (5th Cir. 1984)).

disclosure is made without “reasonable precautions to ensure [the information’s] secrecy.”³⁰ Thus, “[i]f a voluntary disclosure occurs in a context that would not ordinarily occasion public exposure, and in a manner that does not carelessly exceed the imperatives of a beneficial transaction, then the disclosure is properly limited and the requisite secrecy retained.”³¹ Likewise, disclosure does not destroy the information’s secrecy where the owner establishes “a confidential relationship with the other party, by contract or otherwise.” *Southwestern Energy*, 736 F.2d at 597.

Here, there are genuine disputes regarding whether GlobeRanger delivered the Navy Solution to the Navy with adequate precautions to ensure the secrecy of its proprietary information. Again, the Court already concluded that the Navy did not have the undisputed right to disclose the Navy Solution to SAG. And though no evidence shows an express contract between the Navy and GlobeRanger, the summary judgment record reveals various other protections GlobeRanger put in place to maintain the secrecy of its information and create confidential relationships with those who ultimately passed the Navy Solution on to SAG. For example, GlobeRanger protects its RFID solutions, including the Navy Solution, with device-specific license keys that are “node-locked, meaning that once a license file is activated, the software cannot be moved to a different device, or the program will lock, and the user cannot gain access without activation of a new license.” (Pl.’s Resp. 7 (citing Pl.’s App. 426).) GlobeRanger also mandates that employees sign NDAs along with exit certifications and requires contractors—including those working on the Navy Solution—to sign

³⁰ *Interlox Am. v. PPG Indus., Inc.*, 736 F.2d 194, 202 (5th Cir. 1984) (citing *E.I. duPont deNemours & Co. v. Christopher*, 431 F.2d 1012, 1015 (5th Cir. 1970)).

³¹ *Taco Cabana Int’l, Inc. v. Two Pesos, Inc.*, 932 F.2d 1113, 1124 (5th Cir. 1991) (“[T]he disclosure of Taco Cabana plans to contractors did not extinguish their secrecy.”) (citing *Metallurgical Industries*, 790 F.2d at 1200; *International Election Systems Corp. v. Shoup*, 452 F.Supp. 684, 707–08 (E.D. Pa.1978); *Nucor Corp. v. Tennessee Forging Steel Service, Inc.*, 476 F.2d 386, 390 (8th Cir.1973)).

similar NDAs. Further, upon delivering new license keys to the Navy's contractors, GlobeRanger reminded recipients that the keys were to be used "for direct support of the Navy's existing installation of GlobeRanger's Software and for no other purpose and otherwise subject to the terms of the GlobeRanger [EULA]." (Pl.'s App. 238–41.) Similarly, the technical manuals that GlobeRanger delivered had a clear disclaimer that "[d]isclosure outside of GlobeRanger and its suppliers is prohibited." (Def.'s App. 341.) Simply put, the evidence does not indisputably show that GlobeRanger made an "unrestricted disclosure of [its] trade-secret information to third parties." *INEOS Grp.*, 312 S.W. at 852. Rather, a jury could reasonably conclude that GlobeRanger delivered the Navy Solution to the Navy with "reasonable precautions to ensure [the] secrecy" of its proprietary information. *Interlox*, 736 F.2 at 202. The Court, therefore, concludes that genuine factual disputes exist with respect to the first element of GlobeRanger's trade secret claim.

ii. *Element 2: Acquisition through breach of confidence or improper means*

The second element requires GlobeRanger to show that SAG acquired the trade secrets "through a breach of a confidential relationship or discovered by improper means." *Alcatel USA, Inc. v. DGI Techs., Inc.*, 166 F.3d 772, 784 (5th Cir. 1999). To show a breach of confidence, "no express agreement is necessary, but . . . the confidence reposed in the other person must, in some way, be manifest—if not by words, then by the acts of the parties or the whole picture of their relationship." *Furr's Inc. v. United Speciality Advertising Co.*, 385 S.W.2d 456, 459 (Tex. App. 1964) (citing *Hyde Corp. v. Huffines*, 158 Tex. 566 (1958)). Improper means is a catch-all concept that imposes liability on defendants for acts that "include theft, fraud, unauthorized interception of communications, inducement of or knowing participation in a breach of confidence, and other means either wrongful in themselves or wrongful under the circumstances of the case." *Wellogix*, 716 F.3d at 876 (quoting

Astoria Indus. of Iowa, Inc. v. SNF, Inc., 223 S.W.3d 616, 636 (Tex. App. 2007)).

GlobeRanger presents evidence showing three primary instances in which the Navy or its contractors received information from GlobeRanger that contained, or facilitated SAG's acquisition of, GlobeRanger's trade secrets.³² First, in mid-2009, a series of emails originating with Navy's Robert Bacon resulted in GlobeRanger issuing a new license key that made its way to a RAVE team member (Naniq) who later confirmed a fully functioning image of the Navy Solution's server at K-BAY had been made.³³ When GlobeRanger delivered the key, it reminded the recipients that the key was to be used solely for the operation of GlobeRanger's existing solution and subject to the terms of its EULA. Second, in January 2010, the RAVE team (via Naniq) represented to GlobeRanger that it needed another license key for the Navy Solution at Pearl Harbor to conduct maintenance. But in reality, the RAVE team used the key to generate a second fully-functional image of the Navy Solution. RAVE Project team records later show these images were being studied to replicate GlobeRanger's RFID technology using SAG's webMethods as a base. Third, GlobeRanger's delivery of its technical manuals also facilitated SAG's access to GlobeRanger's trade secrets. The manuals had a clear disclaimer on the front cover, instructing readers that disclosure of the information to third parties is prohibited. Because the Court previously found that the Navy did not have the right, as a matter of law, to disclose these items, a reasonable juror could conclude that SAG's acquisition of the trade secrets was improper or entailed a breach of confidence.

Nonetheless, SAG contends that it cannot be held liable for the trade secrets it acquired,

³² Since it finds these to be sufficient for the second element, the Court need not consider the parties' dispute regarding SAG's acquisition of the secrets through Miller, Naniq, and Main Sail.

³³ The evidence the Court relies on here is cited in detail in the Background section, *supra*.

because it was unaware that the Navy did not hold the proper licenses in the Navy Solution. Since SAG indirectly acquired the trade secrets, it cannot be held liable unless it “learned the secret from a third person with notice of the facts that it was a secret and that the third person's disclosure of it was otherwise a breach of his duty to [another].” *Metallurgical Indus*, 790 F.2d at 1204 (quoting RESTATEMENT (FIRST) OF TORTS § 757(c)). GlobeRanger need not, however, show SAG actually knew its acquisition of the trade secrets was improper. Rather, it is enough if SAG should have known of the impropriety of its acquisition, meaning “from the information which [SAG] ha[d], a reasonable man would infer the facts in question, or if, under the circumstances, a reasonable man would be put on inquiry and an inquiry pursued with reasonable intelligence and diligence would disclose the facts.” *Id.* (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt.1).

Here, GlobeRanger submitted sufficient evidence for a reasonable juror to conclude that SAG, at the very least, was on inquiry notice of the facts that the Navy Solution contained GlobeRanger’s trade secrets and that the Navy and its contractors did not have the undisputed right to disclose those trade secrets. GlobeRanger highlights testimony from SAG’s executive admitting its employees “had access to see [GlobeRanger’s] software” and workflows “captured in the GlobeRanger solution for purposes of understanding what the Navy wanted [SAG] workflows to look like when [SAG] replaced the GlobeRanger solution.” (Pl.’s Resp. 29 (quoting Pl.’s App. 219).) Being experienced government contractors, SAG should have at least known to inquire into whether the Navy had the proper license rights to this RFID technology. Even more, SAG had just finished directly competing with GlobeRanger for the precise Navy contract SAG was performing under when it was handed its competitor’s intellectual property to reverse-engineer. And this was just one of the multiple government contracts throughout 2009 and 2010 that SAG and GlobeRanger competed

for. (See Pl.'s App. 420.) Although certain evidence suggests SAG reasonably thought the Navy had the right to disclose the Navy Solution, GlobeRanger has at least made out a *prima facie* case regarding SAG's knowledge of the impropriety of its trade secret acquisition.

In conclusion, a number of genuine factual issues remain with respect to the first two disputed elements of GlobeRanger's trade secret misappropriation claim. Among others, these genuine disputes include: the characterization of the Navy Solution under DFARS; whether the Navy was permitted to disclose the Navy Solution under DFARS; whether GlobeRanger's proprietary information was sufficiently "secret"; the lawfulness of SAG's acquisition of GlobeRanger's trade secrets; and SAG's notice of the impropriety of its trade secret acquisition. In light of the above, the Court **DENIES** SAG's Motion to the extent it seeks summary judgment on GlobeRanger's trade secret misappropriation claim.

B. Tortious Interference with an Existing Contract

Next, SAG challenges GlobeRanger's tortious interference with an existing contract claim. To establish this claim under Texas law, GlobeRanger must prove the following elements: "(1) an existing contract subject to interference, (2) a willful and intentional act of interference with the contract, (3) that proximately caused the plaintiff's injury, and (4) caused actual damages or loss." *Prudential Ins. Co. of Am. v. Fin. Review Servs., Inc.*, 29 S.W.3d 74, 77 (Tex. 2000) (citing *ACS Investors, Inc. v. McLaughlin*, 943 S.W.2d 426, 430 (Tex.1997)).

GlobeRanger presents two theories of liability here. First, it claims that SAG interfered with its contract with the Navy by causing the Navy to violate the terms of GlobeRanger's EULA. Second, GlobeRanger maintains that SAG similarly interfered with its confidentiality agreements with Jason Miller, Naniq, and Main Sail. The Court addresses each theory in turn.

1. Interference with the EULA between GlobRanger and the Navy

SAG argues that GlobRanger cannot show it interfered with any contract GlobRanger had with the Navy, because “there is no evidence that GlobRanger had a valid contract with the Navy.” (Def.’s Mot. 38.) In support, SAG submits that (a) GlobRanger admittedly “never entered into a contract directly with the Naval Supply Systems Command office,” and (b) “there is no evidence that the Navy’s designated contracting officer reviewed and consented to GlobRanger’s EULA” as required by government contract regulations. (*Id.* at 38, 39 (quoting Def.’s App. 478).)

GlobRanger counters that DFARS’s commercial computer software regulations “*automatically*” bind the Navy to the EULA “unless [the Navy] negotiate[s] other rights.” (Pl.’s Resp. 39 (emphasis in original).) GlobRanger maintains that it “is not obligated to demonstrate that anyone at the Navy (and certainly not a contracting officer) *clicked* the EULA themselves.” (*Id.* at 40 (emphasis in original).) Unlike the disputes discussed above, this one is purely legal, and thus, ripe for consideration at this stage in the proceedings.

“It is axiomatic that a cause of action for tortious interference with a contract will not lie in the absence of a contract.” *S & A Marinas, Inc. v. Leonard Marine Corp.*, 875 S.W.2d 766, 768 (Tex. App. 1994). GlobRanger, thus, cannot “sustain a cause of action for tortious interference with a contract,” without proof of “a valid, existing contract subject to interference.” *Gillum v. Republic Health Corp.*, 778 S.W.2d 558, 565 (Tex. App. 1989). GlobRanger has failed to present any evidence in support of this essential requirement.

As an initial matter, GlobRanger has a subcontractor relationship with the Navy, and “it is well-established that subcontractors normally are not in privity with the Government except where the prime contractor is a mere government agent.” *Central Freight Lines, Inc. v. United States*,

87 Fed. Cl. 104, 108 (Fed. Cir. 2009) (citation omitted). “In the absence of such agency, courts have routinely held that a subcontractor has no standing or contractual cause of action to sue the government.” *Id.* (citations omitted). It is undisputed that GlobeRanger never directly entered into a contract with the Navy. GlobeRanger also does not claim that SAIC was a mere agent of the Navy. GlobeRanger’s only assertion here is that DFARS’s commercial software regulations automatically bind the Navy to the EULA’s terms. This argument, however, does not comport with the law.

The DFARS’s provision GlobeRanger relies on states that “[c]ommercial computer software . . . shall be acquired under the licenses customarily provided to the public unless such licenses are inconsistent with Federal procurement law or do not otherwise satisfy user needs.” 48 C.F.R. § 227.7202–1(a). GlobeRanger points to the “shall be acquired” language of this subsection as proof that the government is automatically bound to a contractor’s commercial license the moment that contractor delivers commercial computer software. But there is no reason to believe that this is the intent of DFARS’s “shall be acquired” language.

Consider the context of this language—it falls under section –1 of DFARS § 227.7202, which covers the DoD’s “Policy” regarding commercial computer software acquisitions. Subsection (a), which GlobeRanger relies on, states this policy: commercial software “shall be acquired” under the contractor’s standard commercial license, “unless such licenses” do not fit with the government’s needs. By inserting “shall be acquired” in the beginning of this subsection, the DoD makes its policy clear: assure commercial software contractors that DoD contract officers generally must (“shall”) agree to the terms of the contractor’s commercial license so that such contractors are encouraged

to work with DoD entities without fear of being subjected to DFARS's harsh, default licenses.³⁴ Put differently, this mandatory language tells "the contractor and Contracting Officer" that they are "*supposed* to use the contractor's commercial license."³⁵ However, contrary to GlobeRanger's suggestions, the words "shall be acquired" do not serve as a blanket acceptance on the DoD's behalf anytime a contractor delivers commercial computer software. To find otherwise would render the caveat in subsection (a)—"unless such licenses are inconsistent with Federal procurement law or do not otherwise satisfy user needs"—meaningless. After all, if the government were truly bound to a commercial license it never even gets to review, then it would never be able to determine if an inconsistency with other procurement provisions exists or if the license satisfies user needs.³⁶ Similarly, the commercial software provisions mandating that the government "must negotiate" for any additional rights it needs would also be superfluous. *Id.* § 227.7202–3(b). In short, a fair reading of DFARS § 227.7202–1(a) is that it sets out the rules by which GlobeRanger, SAIC, and the Navy *should have* agreed to limit the Navy's rights, but it does not relieve GlobeRanger of its obligation to show that the Navy actually agreed to the terms of its EULA.³⁷

³⁴ See Dugan, *supra*, at 472 (discussion the policy behind the commercial software regulations).

³⁵ See W. Jay DeVecchio, *Rights in Technical Data & Computer Software Under Government Contracts: Key Questions & Answers*, 12-6 Briefing Papers 1, 4 (2012) (emphasis added).

³⁶ See Trend, *supra*, at 324 (noting the government "cannot accept the commercial license" in certain circumstances).

³⁷ See OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, & LOGISTICS, *INTELLECTUAL PROPERTY: NAVIGATING THROUGH COMMERCIAL WATERS* 30 (2001), available at <http://www.acq.osd.mil/dpap/docs/intelprop.pdf> ("DoD takes the rights customarily offered to the public . . . unless those rights do not meet DoD's minimum needs or violate Federal procurement law. In all cases, a copy of the standard commercial license or any SNLR must be attached to the contract [before the DoD may be bound to its terms]."); Mayner, *supra*, at 24 (explaining how an "end-user license agreement" can be "placed inside the shrink wrap," as well as "into the software" to ensure

In addition to being unsupported by the DFARS provision at issue, GlobeRanger's argument runs contrary to other government contracting regulations applicable in these circumstances. As a general matter, government "[c]ontracts may be entered into and signed on behalf of the Government only by contracting officers."³⁸ 48 C.F.R. § 1.601. The prime contract between SAIC and the Navy reinforce this rule by providing that "[t]he Contracting Officer is the only person authorized to approve changes in any requirements of this contract." (Def.'s App. 226.) These clear mandates would undeniably be violated if the Court were to adopt GlobeRanger's argument and find the Navy is bound to an agreement it never agreed to or authorized others to agree to on its own behalf. At the very least, it would seem that the Navy needs to receive some notice of the EULA before it can be bound by its terms.³⁹ But here, there is no evidence the Navy ever saw the EULA, much less reviewed and agreed to its terms. Similarly, there is no evidence that any contractor acting on the Navy's behalf agreed to the EULA. Indeed, the EULA that GlobeRanger supposedly attached to its software could have just as well been "clicked"—that is, agreed to—by its own employees as they helped implement the Navy Solution. Under these circumstances, the Court has no reasonable basis to conclude that the Navy agreed to be bound by the EULA's terms.

2. Interference with Agreements with Miller, Naniq, and Main Sail

acceptance).

³⁸ GlobeRanger refers to this as a "special rul[e] of government contract formation." (Pl.'s Resp. 39.) But this FAR provision is not simply for "special" circumstances. In fact, this clause falls under FAR's "General" rules for, among other things, "Contracting Authority, and Responsibilities."

³⁹ Cf. DeVecchio, *supra*, at 4 ("[I]f the primes are not forwarding subcontractors' commercial licenses, the prime contractor is not doing what it is supposed to do. And if the prime will not forward the information, then the subcontractor should send it directly to the Government, while also making sure that the subcontract agreement with the prime incorporates the subcontractor's commercial license").

GlobeRanger argues, alternatively, that “even if SAG had not tortiously interfered with GlobeRanger’s EULA, SAG interfered with GlobeRanger’s confidentiality agreements with Jason Miller, Naniq, and Main Sail.” (Pl.’s Resp. 40.) As SAG points out, this theory of liability “is completely absent from the Complaint, which expressly limits GlobeRanger’s tortious interference claim to contracts between GlobeRanger and the Navy.” (Def.’s Reply 22.) Accordingly, SAG asserts that “this claim is not appropriate for consideration.” (*Id.*) The Court agrees.

It is within this Court’s discretion to “disregard claims or theories of liability not present in the complaint and raised first in a motion opposing summary judgment.” *De Franceschi v. BAC Home Loans Servicing, L.P.*, 477 F. App’x 200, 204 (5th Cir. 2012) (unpublished); *see also Cutrera v. Bd. of Sup’rs of Louisiana State Univ.*, 429 F.3d 108, 113 (5th Cir. 2005). Here, as pointed out by SAG, GlobeRanger’s assertion that SAG interfered with the confidentiality agreements signed by Jason Miller, Naniq, and Main Sail is completely absent from the FAC.⁴⁰ Moreover, GlobeRanger stated in its interrogatories that its “claim is based upon Defendants’ actions in causing the breach of various provisions of GlobeRanger’s EULA.” (Def.’s App. 469.) Thus, SAG’s first notice of GlobeRanger’s new theory was in GlobeRanger’s Response to SAG’s Motion for Summary Judgment. This is not sufficient. GlobeRanger cannot “avoid summary judgment . . . by relying on allegations that” SAG interfered with “other contracts” that GlobeRanger never mentioned until now. *Days Inn Worldwide, Inc. v. Sonia Investments*, No. 3:04-cv-2278, 2006 WL 3103912, at *17 (N.D. Tex. Nov. 2, 2006). Therefore, the Court declines to consider whether GlobeRanger’s alternative theory of liability satisfies its tortious interference with a contract claim.

⁴⁰ (See FAC ¶ 107 (“Plaintiff had a valid contract(s) with Navy AIT . . .”).)

In conclusion, GlobeRanger's tortious interference claim fails as a matter of law, because (a) GlobeRanger did not establish the existence of a contract between it and the Navy, and (b) the only other contracts GlobeRanger submits are not appropriate for the Court to consider, for the first time, in ruling on SAG's Motion. Thus, the Court **GRANTS** SAG summary judgment with respect to GlobeRanger's tortious interference with a contract claim.

C. *Unfair Competition and Conspiracy*

SAG's summary judgment assertions regarding GlobeRanger's unfair competition and conspiracy claims can be quickly dismissed on similar grounds. For the unfair competition claim, SAG points out that "Texas courts apply trade secrets law" when the plaintiff's trade secret claim is recast "under the 'unfair competition' umbrella." (Def.'s Mot. 36 (citing *Los Cucos Mexican Café, Inc. v. Sanchez*, No. 13-05-578-CV, 2007 WL 1288820, at *2 (Tex. App. May 3, 2007).) Accordingly, SAG argues that summary judgment is appropriate for GlobeRanger's unfair competition claim "for the same reasons that summary judgment is appropriate on GlobeRanger's trade secrets claim." (*Id.*) However, since the Court denied summary judgment on GlobeRanger's trade secret misappropriation claim, summary judgment is not appropriate for GlobeRanger's unfair competition claim. Likewise, SAG contends that "GlobeRanger cannot succeed on its underlying tort claims and summary judgment is therefore proper on the derivative conspiracy claim." (*Id.*) But again, the Court upheld GlobeRanger's trade secret misappropriation claim, and therefore, summary judgment is not proper for GlobeRanger's derivative conspiracy claim.⁴¹ Accordingly, the Court **DENIES** SAG's Motion to

⁴¹ See *Arthur W. Tifford, PA v. Tandem Energy Corp.*, 562 F.3d 699, 709 (5th Cir. 2009) ("A defendant's liability is derivative of an underlying tort; without independent tortious conduct, there is no actionable civil conspiracy claim.").

the extent it seeks summary judgment on these two claims.

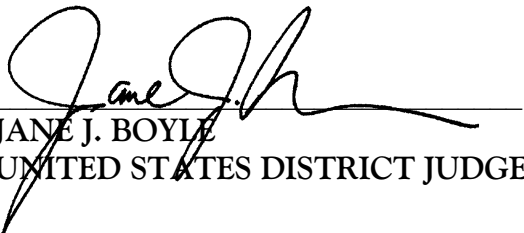
IV.

CONCLUSION

For the foregoing reasons, the Court finds genuine issues of material fact exist for GlobeRanger's trade secret misappropriation, unfair competition, and conspiracy claims. It concludes, however, that summary judgement is appropriate with respect to GlobeRanger's tortious interference with an existing contract claim, because GlobeRanger's failed to establish the existence of a contract that SAG interfered with. Therefore, the Court **GRANTS IN PART** SAG's and Naniq's Motions for Summary Judgment (docs. 135, 138) with respect to GlobeRanger's tortious interference with an existing contract claim and **DENIES IN PART** SAG's and Naniq's motions to the extent they seek summary judgment on GlobeRanger's other three claims. Further, the Court **DISMISSES WITH PREJUDICE** Count IV (tortious interference with an existing contract) of GlobeRanger's First Amended Complaint (doc. 79).

SO ORDERED

SIGNED: June 20, 2014.



JANE J. BOYLE
UNITED STATES DISTRICT JUDGE